

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division**

UNITED STATES OF AMERICA)	
)	
)	Case No. 3:19cr130
)	
OKELLO T. CHATRIE,)	
Defendant)	

NOTICE OF SUPPLEMENTAL AUTHORITY

Okello Chatrie, through counsel, hereby advises the Court of new authority regarding the unconstitutionality of “geofence warrants.” In *Commonwealth v. Fleischmann*, a Massachusetts trial court held that a geofence warrant was overbroad and suppressed the fruits of the search under the Fourth Amendment and the Massachusetts Declaration of Rights. *See* Ex. A, Memorandum of Decision and Order on Defendant’s Motion to Suppress Search Warrant, *Commonwealth v. Fleischmann*, No. 2072CR00046 (Ma. Sup. Ct. Aug. 31, 2021).

Fleischmann involved a geofence warrant issued to Google in connection with a home invasion investigation. Step 1 sought “anonymized” Location History data for two locations over the course of two hours: (1) 50 meters around the home and (2) 100 meters around another location of unexplained significance. *See id.* at 3-4, 11 n.7. Step 2 authorized the police to unilaterally request additional location data outside of the geofences for devices “deemed relevant.” *Id.* at 4. And for those devices, the warrant further authorized police to obtain various types of subscriber information identifying the account holders as well as six months of internet protocol (“IP”) address history. *Id.*

The court first determined that *Fleischmann* had standing to challenge evidence obtained from an “improper ‘general’ warrant.” *Id.* at 7-8. It then found that the “third-party doctrine” does not apply and that a warrant is required to access Google location data. Although Massachusetts

has a “safe harbor rule” that does not require a warrant for six hours or less of “telephone call location data,” the court found that rule inapplicable. *Id.* at 8. The court reasoned that Google location data is different from “telephone call location data,” which only records device location when the user makes or receives a phone call. *Id.* By contrast, the court noted that Google data “is collected continually, regardless of whether a user is actively making or receiving a phone call, as long as a Google-related application exists on their cellular phone.” *Id.* at 9. The court also relied on the warrant’s authorization for six months of IP address information, which “can be used to determine location data.” *Id.* at 10. The court similarly distinguished the six days at issue in *Carpenter v. United States*, 138 S. Ct. 2206, 2217-2220 (2018). *Id.*

Finally, the court determined that the geofence warrant was overbroad under the Fourth Amendment and Article 14 of the Massachusetts Declaration of Rights. *Id.* at 10-11. The court noted that “the initial inquiry appeared narrowly tailored; the warrant was curtailed to a two hour window, with an arguably specific radius to the scene of the crime,” but determined that this was “not the limit of what the warrant authorized.” *Id.* at 11. The court was particularly concerned with the discretion afforded to police in Step 2, allowing them to request additional location data and subscriber information without judicial oversight.¹ Moreover, the court recognized that providing supposedly “anonymized” data in Step 1 was no cure, because the warrant authorized the police to obtain this additional data for “any device” identified in the initial dragnet. *Id.* Consequently, the court found the warrant overbroad and suppressed the “fruits of the poisonous tree,” including information about Fleischmann’s device and statements made as a result of the tainted data. *Id.*

¹ Mr. Chatrue makes a similar argument in the context of the warrant’s lack of particularity in Steps 2 and 3. *See, e.g.*, ECF No. 205 at 37-40.

This is the first written state court decision addressing the constitutionality of a geofence warrant that counsel for Mr. Chatrue is aware of. There remain four federal magistrates who have also considered geofence warrants, and three have likewise found them unlawful. *See In re Search of Information That Is Stored at the Premises Controlled by Google* (“Mitchell Opinion”), No. 21-MJ-5064, 2021 WL 2401925 (D. Kan. Jun. 4, 2021); *In re Search Warrant Application for Geofence Location Data Stored at Google* (“Harjani Opinion”), No. 20 M 525, 2020 WL 6343084 (N.D. Ill. Oct. 29, 2020); *In re Information Stored at Premises Controlled by Google* (“Fuentes Opinion”), 481 F. Supp. 3d 730 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google* (“Weisman Opinion”), No. 20 M 297, 2020 WL 5491763 (N.D. Ill. July 8, 2020).

Respectfully submitted,
OKELLO T. CHATRIE

By: /s/
Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

_____/s/_____.
_____.

Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org